Step 4: Testing the Design and Operating Effectiveness of your Controls

Once you have completed your Inherent Risk Assessment, it is important to then give consideration to **the measures you have in place to mitigate and manage the inherent risks you have identified** (i.e. what is your mitigation plan to address the risks?) This involves three key initial tasks:

1. **Identify your controls – list what you are already doing.** Write down all the things you do to prevent money laundering. You probably have more controls than you think! Common examples include member/visitor checks, gaming controls, staff training and transaction monitoring.

2. **Document your controls**. Many businesses have put in place measures to do the right thing for many years, just not in a formal way. Now is the time to write it down:
   What exactly do you do?
   Who does it?
   When does it happen?
   What records do you keep?
   Where you identify old processes that are no longer used, note that and retire them.

3. **Assign Ownership.** For each control, decide who is responsible. This person will:
   Make sure it is working
   Report any problems
   Sign off that it is effective

Now that you have pulled this important information together, you should look at two key areas:

- **How do you know your control is working on an ongoing basis?** This will help you inform how you determine to **monitor** the control and alert if it isn't working. This is about keeping your finger on the pulse.

- **What risk does the control address? High, medium or low?** This will help inform you how you determine to test the control and at what intervals. E.g. you might test your high-risk controls six monthly, your medium risk annually and your low risk controls every two years.

AUSTRAC provides useful guidance about how to look at risks and conduct risk assessments. For further information, please see here.

Having identified your controls, how do you make sure as a reporting entity the controls address the risk/obligation and are working?

Controls Monitoring

Are your controls working as part of normal ops?

There are different ways you can monitor to make sure that your controls are operating properly. These include (without limitation):

- **Performance metrics and KPIs**. Track simple numbers to tell you if things are working. For example: number of KYCs conducted; number of member ID checks conducted; AML training completion rates; time to conduct ECDD investigations from alert.
- **Sample Testing.** You might institute a quarterly or 6 monthly process where a separate team (for instance, your AML Team) conducts sample testing on the operation of a control. For instance, looking at alerts from the transaction monitoring program and how they have been investigated.
- **Control Gap Analysis.** You might have your compliance team look at your transaction monitoring or another key control and its coverage.
- **Attestation**. You might introduce a process for control owners (at an appropriate cadence for your business based on its Context) to sign off that they have oversight of their controls environment and that it is operating as intended.

Controls Testing

Step back: formally evaluate whether your controls are properly designed and are actually working

There will be certain risk areas (i.e. high ML/TF risk) and obligations where you will want to ensure, at a regular cadence, that you have 'fresh eyes' (whether internal or external) on the design and operation of the control, to make sure that it addresses the risk / obligation and it is operating properly.

You don't want to be seen as marking your own homework!

Testing involves looking at the **design** and the **operating effectiveness of your control.** The process will consider both **quantitative** and **qualitative** considerations.

When looking at the **design** of a control, the testing party will be looking at **what it applies to** (risk or obligation?), whether it is **documented** and can be **evidenced**, how it **operates**, whether it is **reliable** and whether there is relevant prior audit/performance information about the control (e.g. have there been operational issues before?)

When looking at the **operation** of a control, the testing party will be looking at a sample size (referable to the size of your business) to see whether the control has been operating the way it is meant to.

Sample Case Study – Know Your Customer Processes: A hypothetical example

Under Australia's AML laws, XYZ Club Pty Limited (**XYZ**) has conducted its annual **ML/TF Risk Assessment** and a review of its **obligations** as it relates to conducting 'know your customer' checks on its members and guests. At a recent conference, XYZ heard from AUSTRAC and other key intelligence-industry speakers on the importance of obtaining KYC information on members and guests and takes its responsibilities very seriously in this area. Accordingly, XYZ has put in place a number of controls as follows:

- KYC upon registration of all new members, photographs on member cards and member 'tap in' at each visit.
- Identification processes (captured by its system) for guests.
- AML/CTF screening on new members and on gaming patrons at particular thresholds.
- Enhanced customer due diligence for high-value gaming members (including loyalty program members).
- Ongoing monitoring of transaction patterns.
- Staff training.

To ensure that these controls are working, XYZ has put in place a monitoring and testing framework. This framework has been implemented having regard to the size, scale and complexity of its operations, which it identified as part of its ML/TF Risk Assessment process.

Monthly Oversight / Monitoring

- AML Team Key Metrics Reporting to Senior Management and Board on number of KYC conducted, results of AML/CTF Screening, ECDD opened and closed, SMRs lodged, staff training rates.
- Review of all high-risk customers and report on actions taken.
- Any deviations in expected metrics are investigated. Key non-compliances noted, including action taken with relevant staff member under Employee Due Diligence procedures.

Quarterly Controls Monitoring (against set targets established by Board, with sample testing commensurate with the identified ML/TF risk)

- Sample 20 new member applications monthly.
- Sample 20 KYC files for large wins.
- Sample 20 CircleScan files for visitors.
- Verify completeness of ID.
- Check staff adherence to procedure.
- Review of all medium risk customers.

Annual Controls Design and Operating Effectiveness Testing (conducted by an independent party – either internal or external)

- **Sample Testing of KYC processes.**
- **ECDD**: Sample 20 Enhanced Customer Due Diligence files and assess the appropriateness of the risk allocation.
- **CDD**: Review all high-risk customers for the appropriateness of the risk allocation and ongoing business relationship.
- **TMP**: Review of rules and tuning (including to reflect the ML/TF Risk Assessment results).
- **Adherence to Procedures:** Mystery Shopper program implemented.

Where the monitoring picks up issues or control failures (for example, staff seeking a 'workaround' for a control), XYZ will then promptly action them (with oversight of Senior Management) and then monitors them to make sure the issue has been fixed. Having monthly and quarterly processes means that if there is an issue, XYZ is confident that they will identify and rectify it.

Make this work for your business

Start Simple and Build Out

Look at your highest risk areas. Pick 3 – 5 of your most important controls. Set up basic **monthly monitoring** and reporting to your Board / Senior Management Team. Schedule quarterly reviews and plan annual testing for your highest risk areas.

Keep it Proportionate to your Context

Review the work you have done in your ML/TF Risk Assessment. Not all entities are alike, and your monitoring and testing program should accord to the size, scale and complexity of your business.

Document Everything

It is critical that not only is this work done, but that you can prove it was done. Keep records of what you monitor and what you tested, when you tested it, what you found and, where relevant, what you fixed.

Remember: this protects your business.

Good control testing isn't just about compliance - it protects your reputation, your licence and your business. When your stakeholders or the regulator asks you about your risk environment and your mitigation / management plan, you want to confidently say: "Yes, we know our controls work because we monitor and test them regularly."

Need Help?

AUSTRAC has useful guidance materials and please contact LCA.

Lane
Consulting & Advisory

278 Richardson Street
Middle Park, Victoria 3206

0421 671 571

louise@laneconsultingandadvisory.com

https://laneconsultingadvisory.com